Shaping the Future of Aerospace

On TTEthernet for Integrated Fault-Tolerant Spacecraft Networks

Andrew Loveless

NASA Johnson Space Center (JSC)

AIAA SPACE 2015, Aug. 31st – Sep. 2nd 2015

Pasadena, CA

Project Overview and Motivation

- **Integrated modular avionics (IMA) principles are attractive for inclusion in spacecraft architectures.**
  - Consolidates multiple functions to shared computing platforms.
  - Reduces spacecraft cost, weight, and design complexity.
  - Interchangeable components increases overall system maintainability – important for long duration missions!
- **The Avionics and Software (A&S) project**
  - Funded by NASA's Advanced Exploration Systems program.
  - Developing a flexible mission agnostic spacecraft architecture according to IMA principles.
  - NASA can minimize development time and cost by utilizing existing commercial technologies.
  - Matures promising technologies for use in flight projects.

Project Overview and Motivation

- **IMA Considerations in Networking**
  - Requires network capable of accommodating traffic from multiple highly ***diverse systems*** (e.g. critical vs. non-critical) – potentially all from ***one shared computer platform***.
  - Must prevent cascading faults b/w systems of differing criticalities connected to the same physical network.
    - ⚠ Most avionic system failures result from ineffective fault containment and the resulting domino effect.
  - Some network technologies are better suited for certain tasks.
  - Applying the same technology everywhere traditionally results in undue expense and limited performance.

Results in hybrid architectures with multiple technologies (e.g. NASA's LRO has MIL-STD-1553, SpaceWire, LVDS).

Project Overview and Motivation

- **Ethernet is promising**
  - Inexpensive, widespread, and high speed = highly flexible.
  - Commonality promotes interchangeability between components.
  - Can augment with QoS enhancements for critical applications.
  - The A&S project considers Ethernet fundamental in the design of future manned spacecraft.
- **Integrated Power, Avionics, and Software (IPAS)**
  - Flexible evaluation environment for hardware and software in simulated mission scenarios.
  - Realistic framework of vehicle subsystems connected via Ethernet backbone.

Andrew Loveless, NASA/JSC

Ethernet in Space Programs



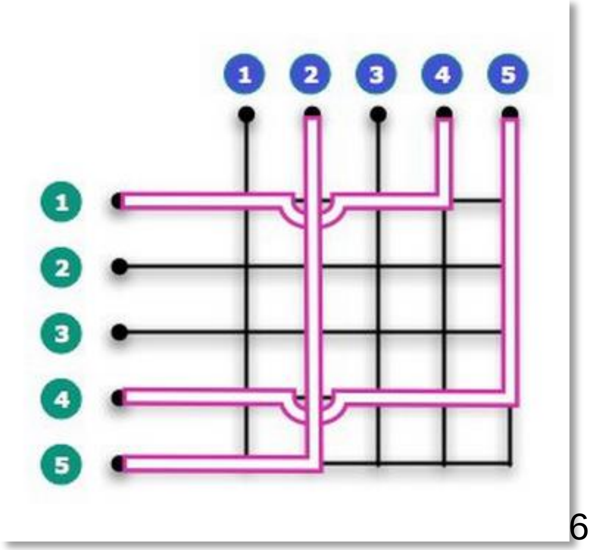






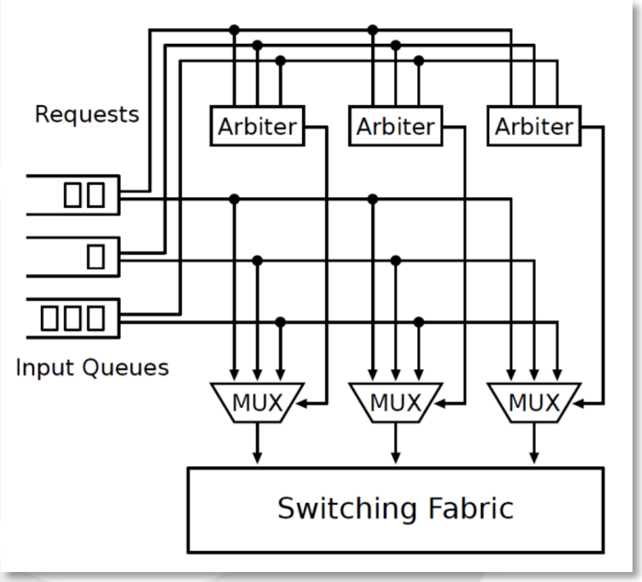
Shortcomings of Classical Ethernet

- **Classical Ethernet characteristics**
  - Event-driven communication – messages are only sent in response to environmental or internal events (asynchronous).
  - Best-effort paradigm – no guarantees regarding transmission time or successful message delivery.
- **Timing within an Ethernet network is not predictable.**
  - Event-triggered = multiple frames will need to travel through the matrix simultaneously.
    - Usually supported by the switch fabric's parallel arrangement (space partitioning).
  - Collisions occur when frames are forwarded simultaneously to the same output port.
  - Arbitration is needed to regulate input to the switch fabric.



Shortcomings of Classical Ethernet

- **What factors impact forwarding delay?**
  - 1) Degree of contention, 2) arbitration method
  - Frequency/severity of conflicts is highly variable.
- **Contention limits throughput**
  - Leads to buffer overflows and dropped frames.
  - 58.6% with input FIFOs under uniform traffic.
  - >80% with VOQs, crosspoint buffers, and better arbitration procedures (e.g. matrix, wavefront).



- **Modern advancements don't address unpredictable timing.**
  - E.g. VOQs eliminate head-of-line blocking, but still require arbitration.

Flight critical functions must operate in an entirely predictable manner and require a level of network determinism that classical Ethernet can't provide.

Ethernet for Critical Applications

Quality of Service (QoS): Methods for controlling bandwidth, latency, jitter, or data loss in mission-critical networks (e.g. prioritization, traffic shaping).

- **“Industrial Ethernet” (e.g. ≤100Mbit/s EtherNet/IP, PROFINET)**
  - Replaces proprietary Fieldbus solutions on factory floor (e.g. machinery).
  - Modified w/ master/slave arch., I/O controllers, and bus or ring topology.
  - RT services through specialized HW and extra protocols around payload.
- **Rate-Constrained (e.g. ARINC 664P7-1, IEEE 802.1BA AVB)**
  - Predetermined knowledge of traffic patterns (max size, frequency) ensures upper bound on TX delays.
  - A priori agreement of network devices prevents buffer overflows in switch.
  - Latency 1-10ms, < 500μs jitter, arbitration.

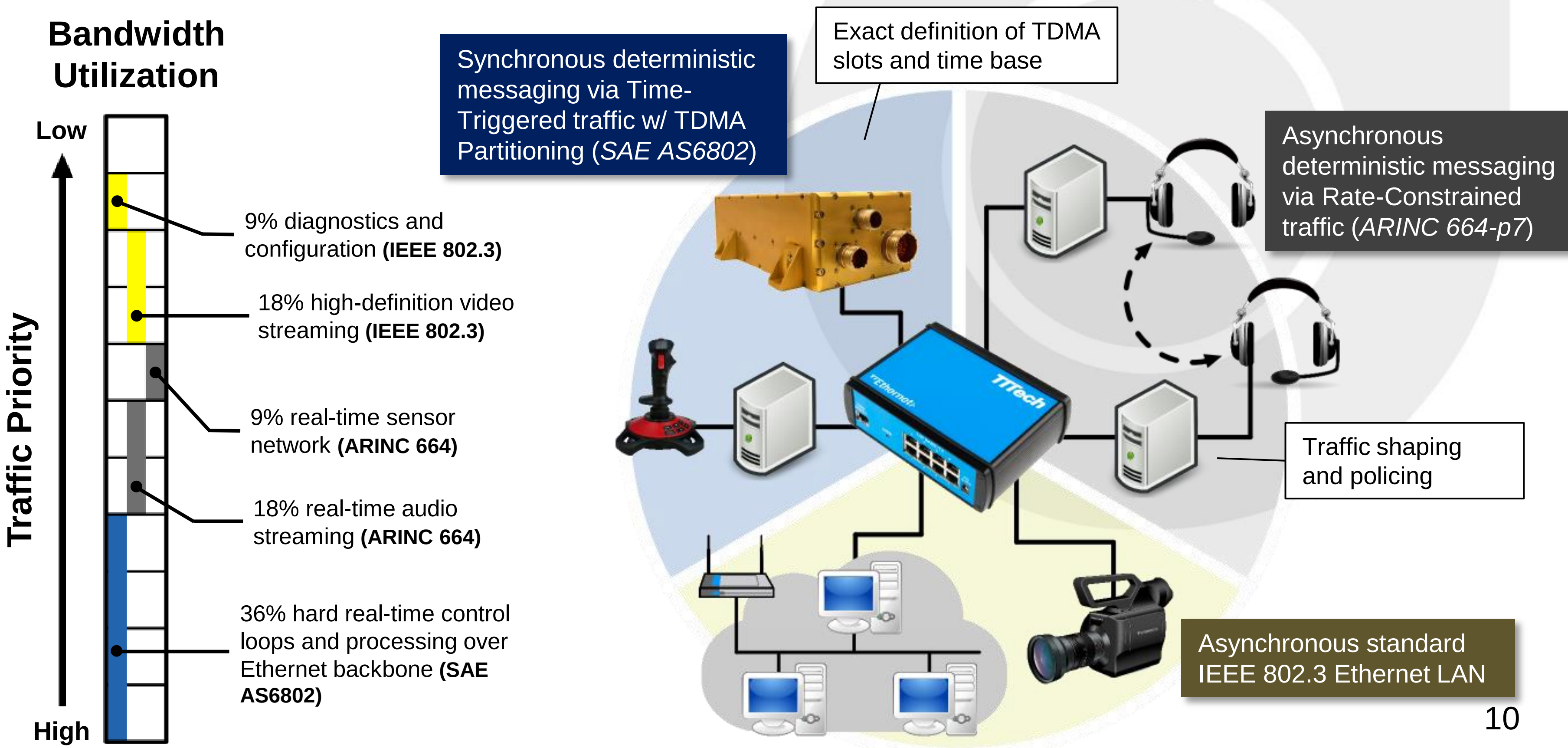
Ethernet for Critical Applications

- **Time-Triggered Ethernet (SAE AS6802)**
  - Uses specialized end systems and network switches (like AFDX).
  - Network planning tool allocates each device a finite transmission window.
  - Each slot is repeated sequentially to form a periodic comm. schedule.
  - Config. files specifying schedule are loaded onto each network device.
- **Eliminating contention = no arbitration**
  - Decentralized synchronization process establishes a global time base.
  - Devices reference time to dispatch messages at predetermined instances.
  - Schedule guarantees no contention between TT frames.
  - Latency < 12.5 μs/switch, < 1μs jitter, <u>no arbitration</u>

> Note that controlling the jitter dramatically lowers latency compared to asynchronous RC traffic. A large portion of latency is the jitter!

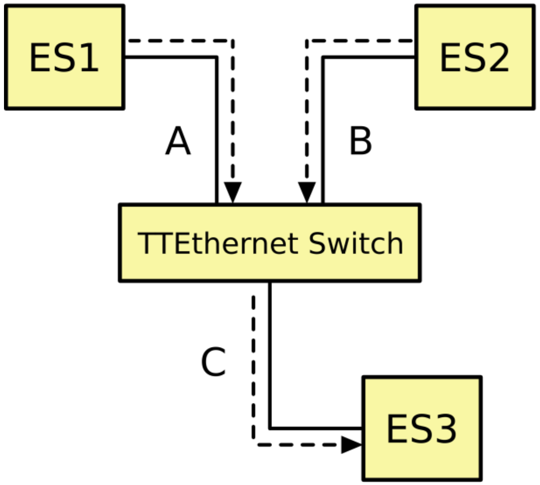
TTEthernet Traffic Integration

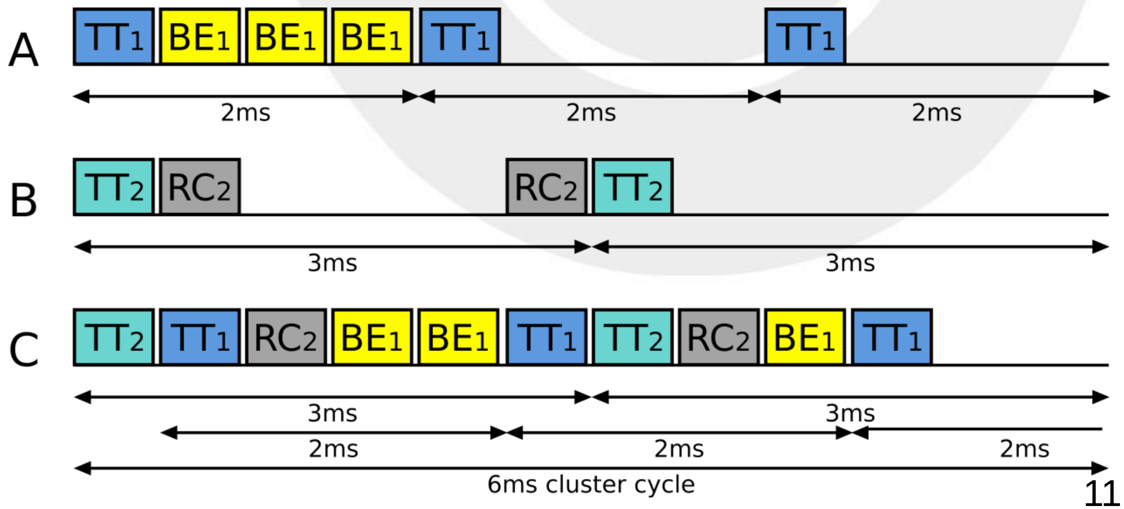
TTEthernet overcomes difficulties in realizing an IMA architecture by providing three distinct traffic classes covering the full spectrum of criticality levels.



TTEthernet Traffic Integration

- **Priority-based partitioning: 3 traffic classes on 1 physical layer.**
  - Messages forwarded: 1) as scheduled (TT), or 2) as priority allows (RC, BE).
  - Bandwidth is released if TT message is not sent in synchronous time slot.
  - Ensuring determinism in a mixed-criticality network:
    - Timely block: Prevents RC or BE transmission during TT slots (unless freed).
    - Shuffling: Higher priority message is queued until lower priority frame is sent.

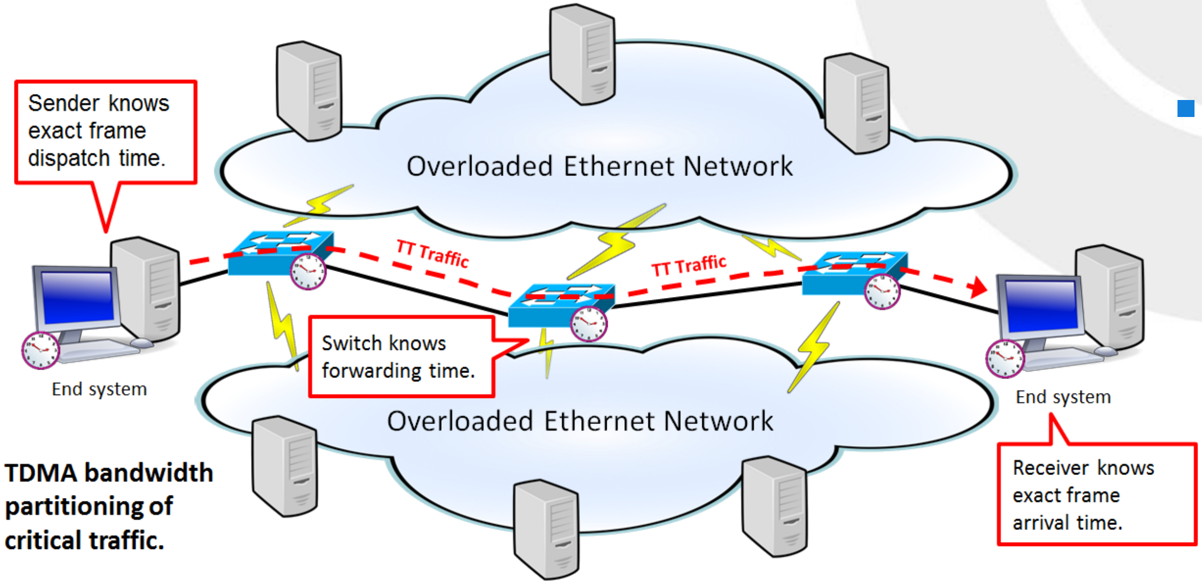




TTEthernet Traffic Integration

TTEthernet network partitioning reduces cascading faults b/w platforms w/o the need for complex fault isolation procedures at the application level.

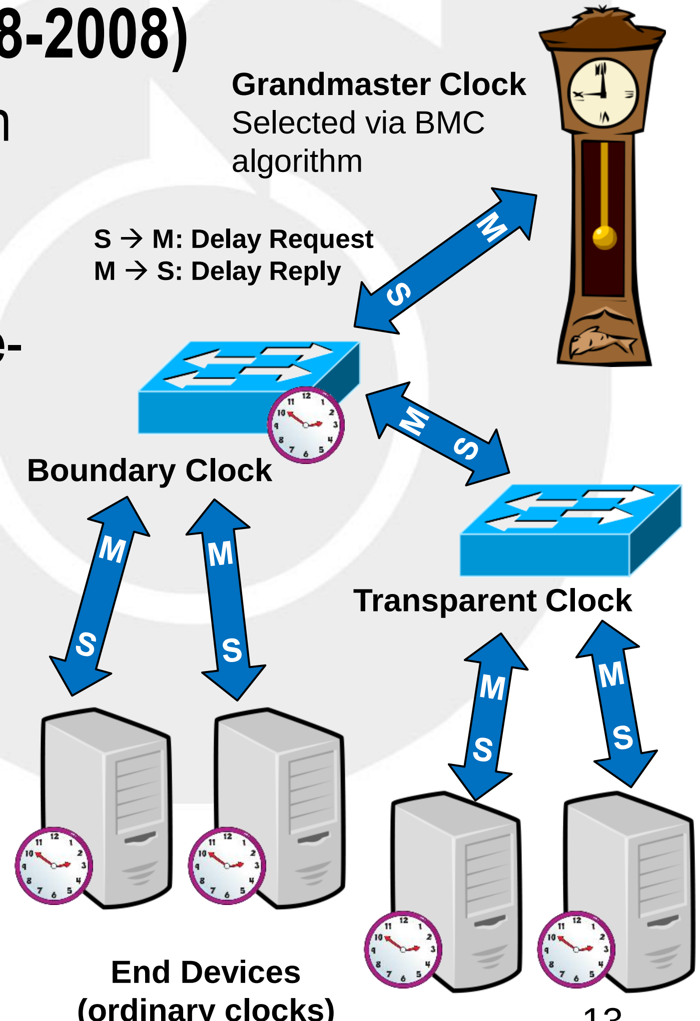
- **Traffic classes provide hard fault containment in the network.**
  - Guaranteed TT frame delivery regardless of asynchronous traffic patterns.
  - Communication schedule controls access of devices to network resources.



- Switches act as central bus guardians to protect against arbitrarily faulty end systems.
  - TT: acceptance window
  - RC: temporal distance

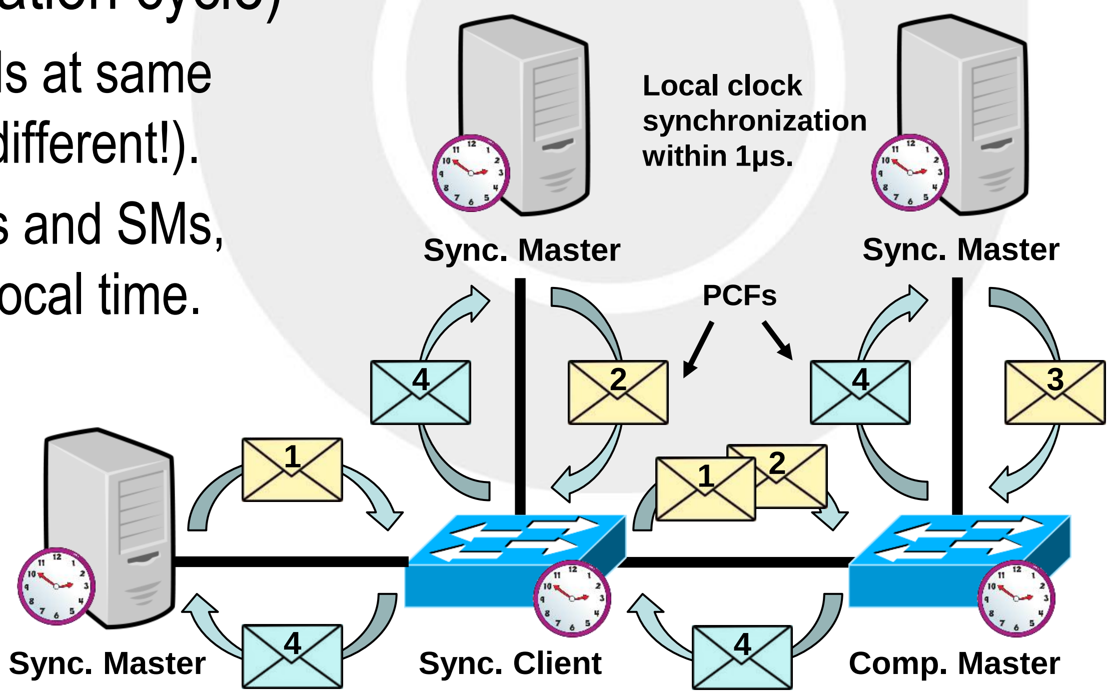
Synchronization Comparison

- **Precision Time Protocol (PTP IEEE 1588-2008)**
  - State-of-the-art Ethernet clock synchronization algorithm in industrial applications.
  - Improves over Network Time Protocol (NTP) through specialized network hardware for time-stamping and decoding (sub-μs accuracy).
  - Protocol can be at Ethernet or IP layers.
  - Hierarchical master/slave arch. for distributing time-of-day and clock frequency information.
  - Uses best master clock (BMC) algorithm to select grandmaster clock source.
  - Built-in redundancy means that if clock source fails, another is selected.



Synchronization Comparison

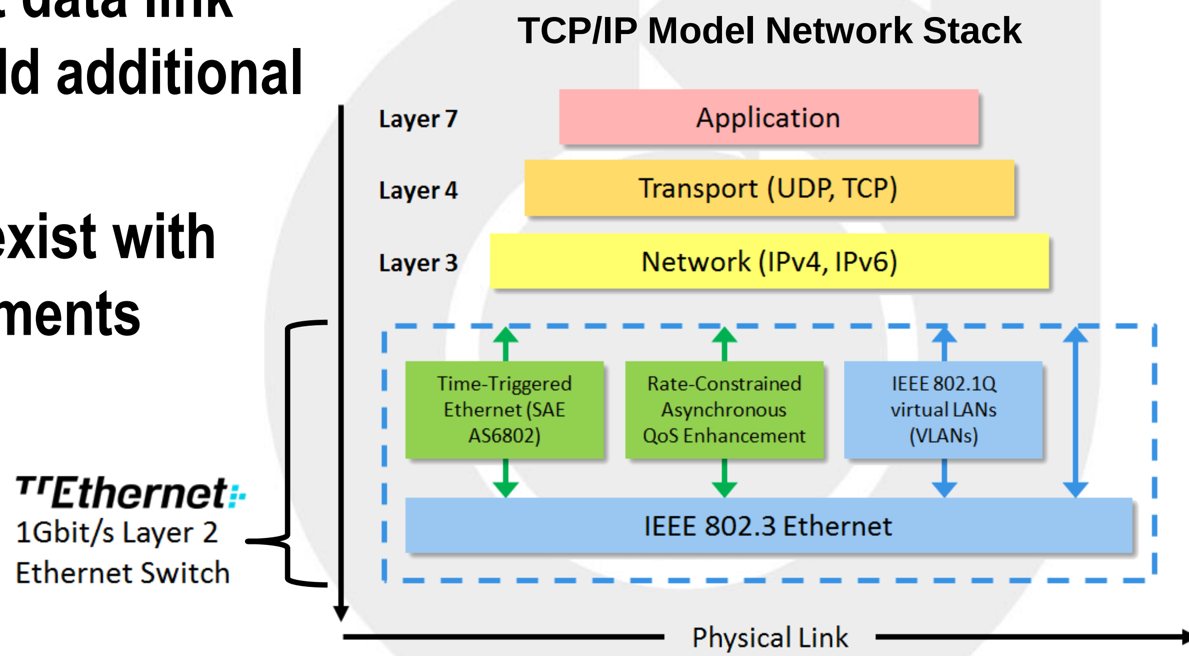
- **Time-Triggered Ethernet (SAE AS6802)**
  - Based on the exchange of asynchronous Protocol Control Frames (PCFs).
  - Each component is assigned one of three roles (SC, SM, or CM).
- Two Step Process (integration cycle)
  - SMs dispatch PCFs to CMs at same local time (drift = actually different!).
  - CMs send PCFs to all SCs and SMs, which they use to correct local time.
- Key Differences
  - Decentralized "master".
  - No search for best clock.
  - Tolerates multiple faults.
  - No external wall clock.



TT/RC Network Stack Integration

- **Directly alters Ethernet data link layer (L2). Does <u>not</u> add additional protocol layers.**
- **Traffic classes can coexist with other L2 QoS enhancements (e.g. IEEE 802.1Q).**

Common higher level protocols (e.g. IPv4, UDP) can be used on top of TTEthernet's data link layer.



IEEE 802.3 (Classical Ethernet)

7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes	12 bytes
Preamble	SFD	Destination Address	Source Address	EtherType (Length)	Data Payload	FCS	IPG

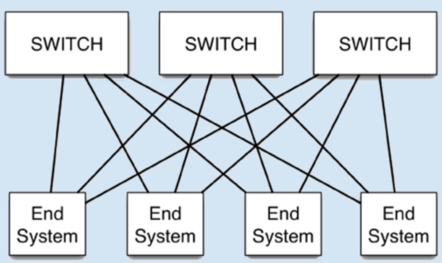
ARINC 664-P7 (RC) SAE AS6802 (TT)

7 bytes	1 byte	4 bytes	2 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes	12 bytes
Preamble	SFD	CT Marker	CTID	Source Address	Length	Data Payload	FCS	IPG

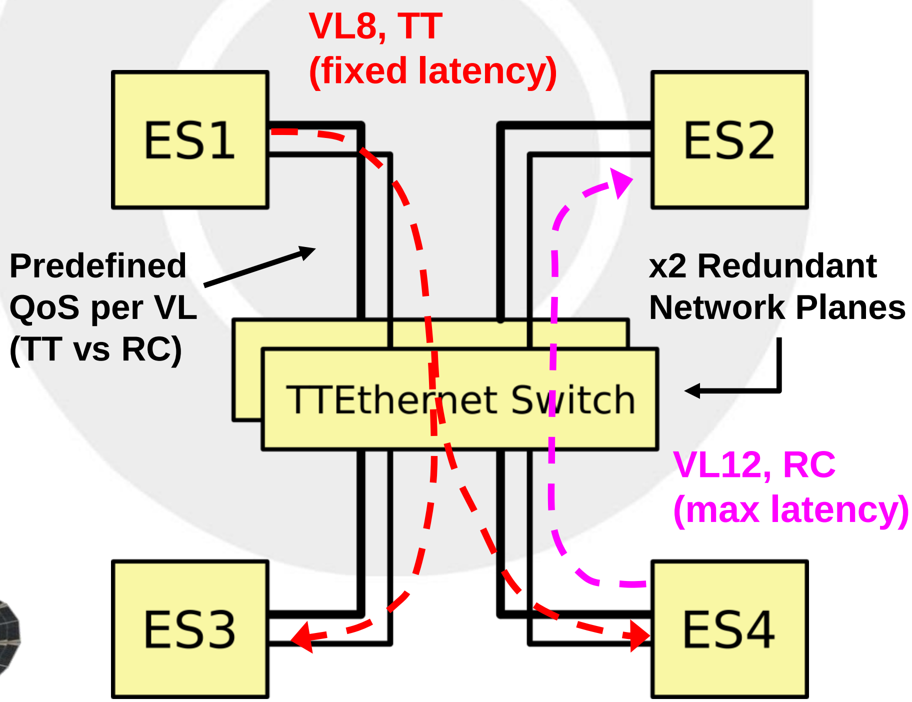
Virtual Links and Redundancy

- **SAE AS6802 (TT) and ARINC 664p-7 (RC) use Virtual Links (VLs) to replace traditional MAC-based message delivery.**
  - Static forwarding table associates VLs with switch output ports.
  - VLs emulate point-to-point wiring seen in federated architectures.

- Increase fault-tolerance with multiple parallel switches.
- Redundancy mgmt. discards extra frames.
- Dual-fault tolerant w/ three redundant channels and high integrity devices.



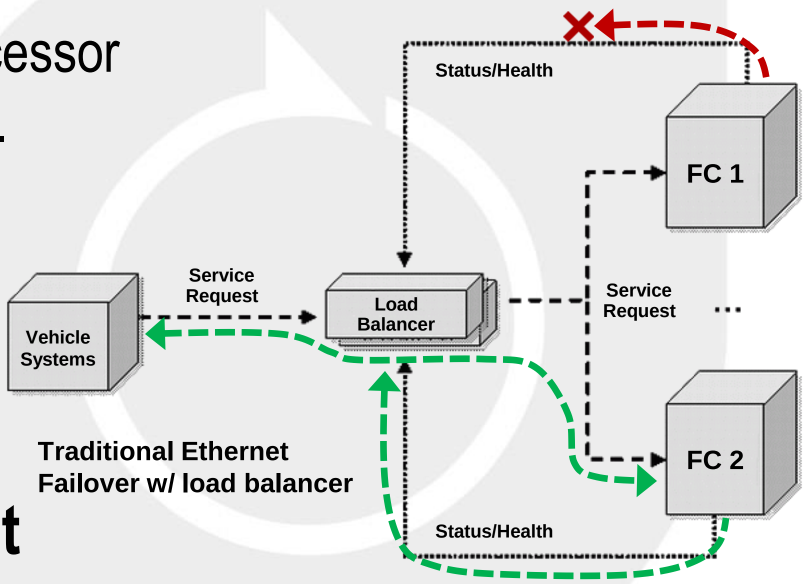
Fail-Operational



Sample TTEthernet Network

Flight Computer Failover

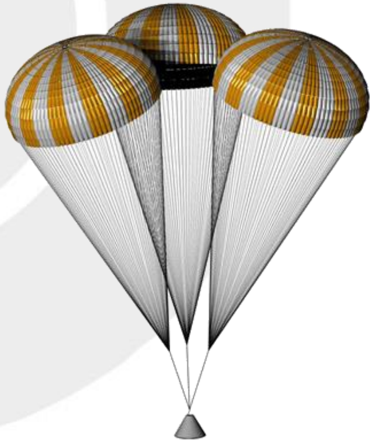
- **Past efforts used classical Ethernet over vehicle backbone.**
  - Load balancer acted as virtual flight processor IP, detecting failure and directing TX/RX.
  - Introduces single point of failure.
  - Can increase fault tolerance w/ VRPP or redundant load balancers.
  - ✗ Relies on monitoring with BE Ethernet.



- **Failover with deterministic Ethernet**
  - Virtual link based delivery removes need for load balancer.
    - Identical messages can be dispatched to multiple recipients simultaneously.
  - Means FC's have access to same data = More seamless failover.
  - Can increase fault tolerance with redundant TTEthernet switches.
  - Schedule driven communication compliments flight software behavior.

Ascent Abort 2 (AA-2) Simulation

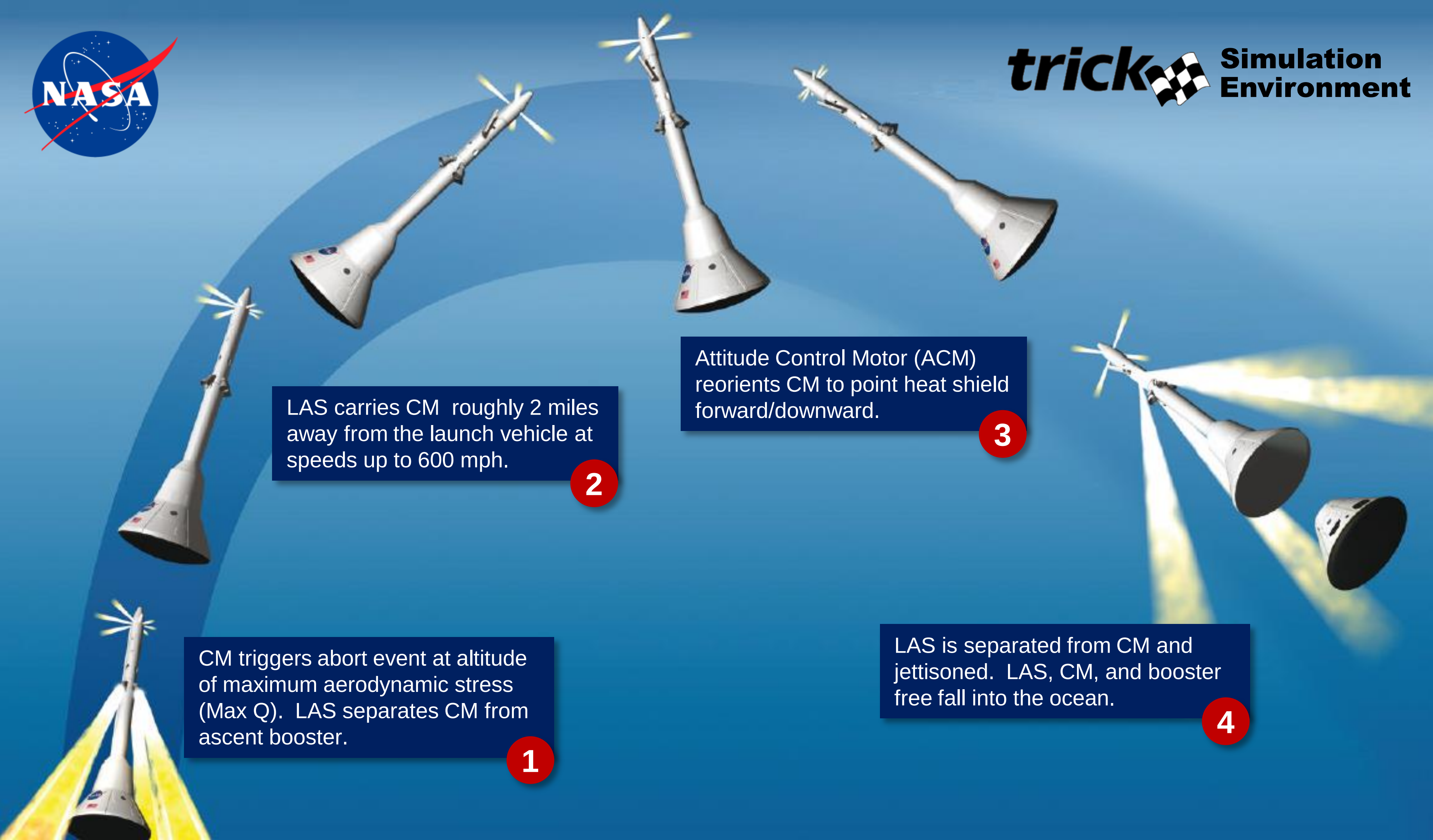
- **What is the Ascent Abort 2 Flight Test?**
  - Launch Abort System (LAS) carries CM away from ascent booster.
  - Goal is to stress the capabilities of synchronized redundant control loop.
  - Conducted AA-2 flight test demo in May ‘15 Integrated Test at JSC.
- **Redundant Flight Computer Architecture**
  - Three identical redundant flight computers (pc-linux).
  - Failover logic built into Core Flight Software System (CFS).
  - Synchronization over TTEthernet network (200Hz).
  - CFS included several genuine Orion fsw components:
    - Absolute Navigation (AbsNav) for Exploration Mission EM-1.
    - Service module abort, stochastic/optical navigation, and propellant balancing.
  - ANTARES simulation integrated into Tricksim.
    - Official NASA Orion spacecraft assessment tool used by JSC’s GNC branch.



Andrew Loveless, NASA/JSC

Ascent Abort 2 (AA-2) Simulation

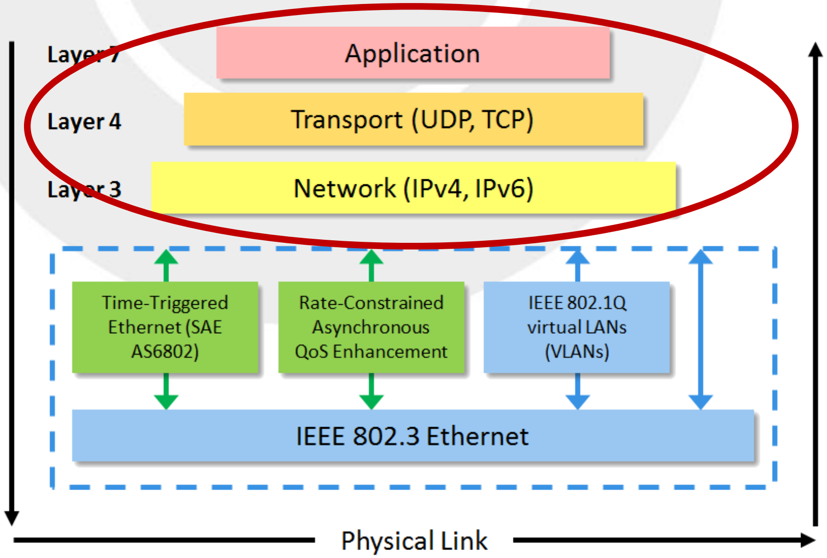
trick Simulation Environment



Software-Level Network Stack

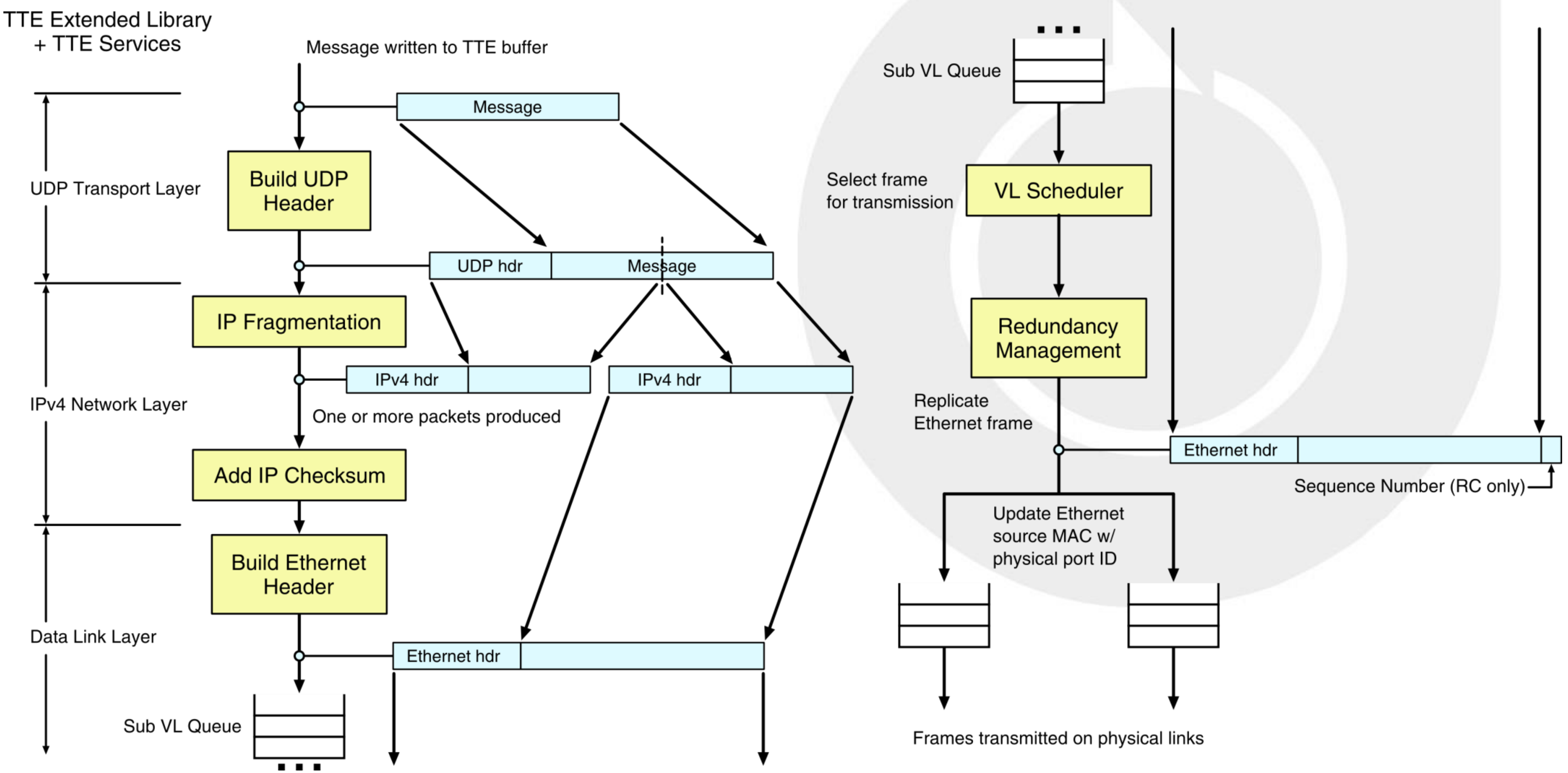
- **AA-2 – Unique Mission Requirements:**
  - Message payload sizes from simulation up to 20,000 bytes.
    - Ethernet frame data length is limited to 1500 bytes.
  - Throughput rates up to 100Mbit/s per Ethernet link.
  - Comm. with classical Ethernet systems w/o separate network adaptor.
- **Extension to TTEthernet Library (Phoenix IP - data link layer):**
  - Implements IPv4 (RFC 791) and UDP (RFC 768) protocol layers.
  - Abstraction from DMA management.
  - Built in software = cross-platform.
  - Maximizes throughput (e.g. minimize copies, parallel checksum summation).

New Network Stack and API



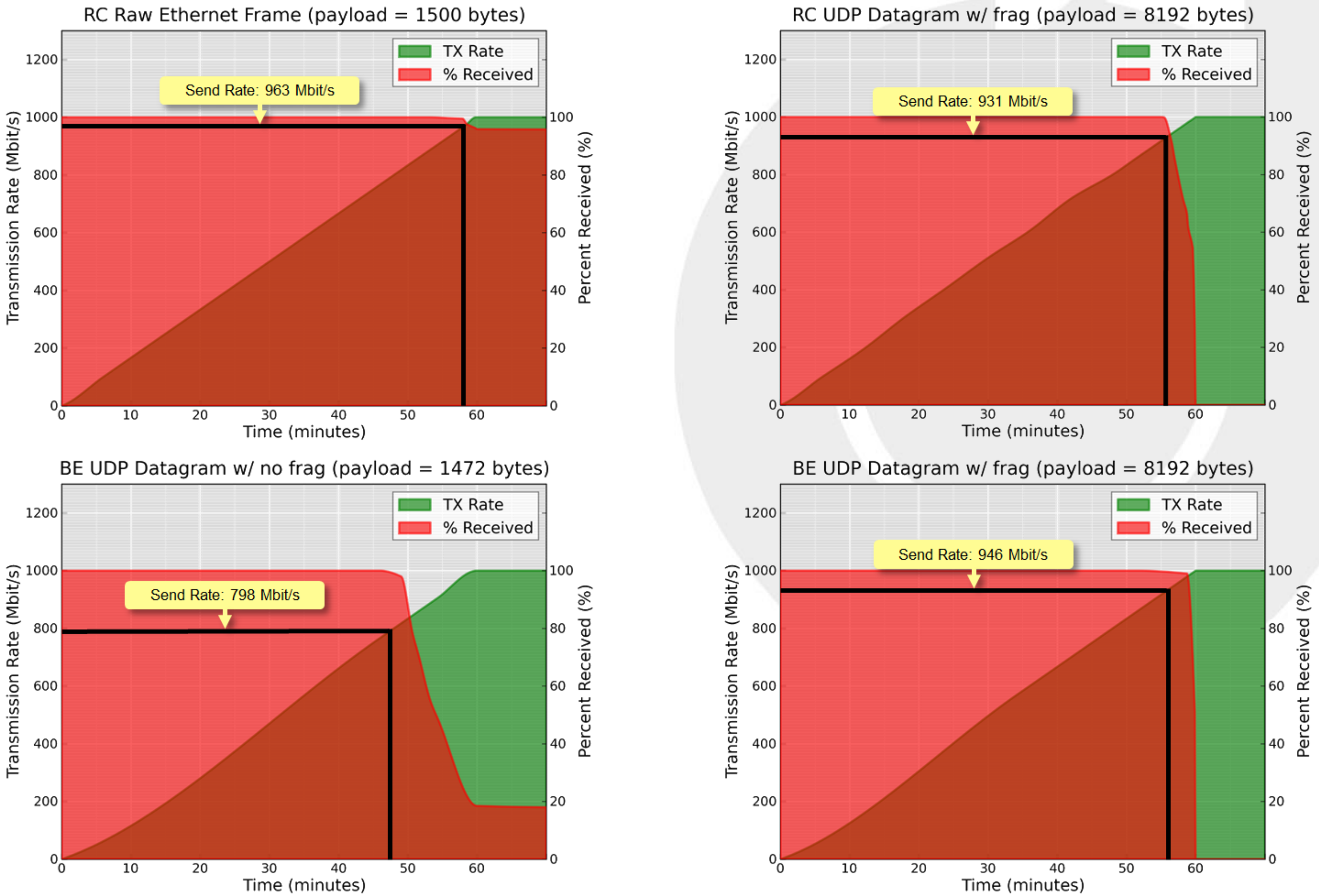
Software-Level Network Stack

65,507 octets supported by library (max UDP data length according to RFC 5405)



TTEthernet Extended Library TX protocol stack

Software-Level Network Stack

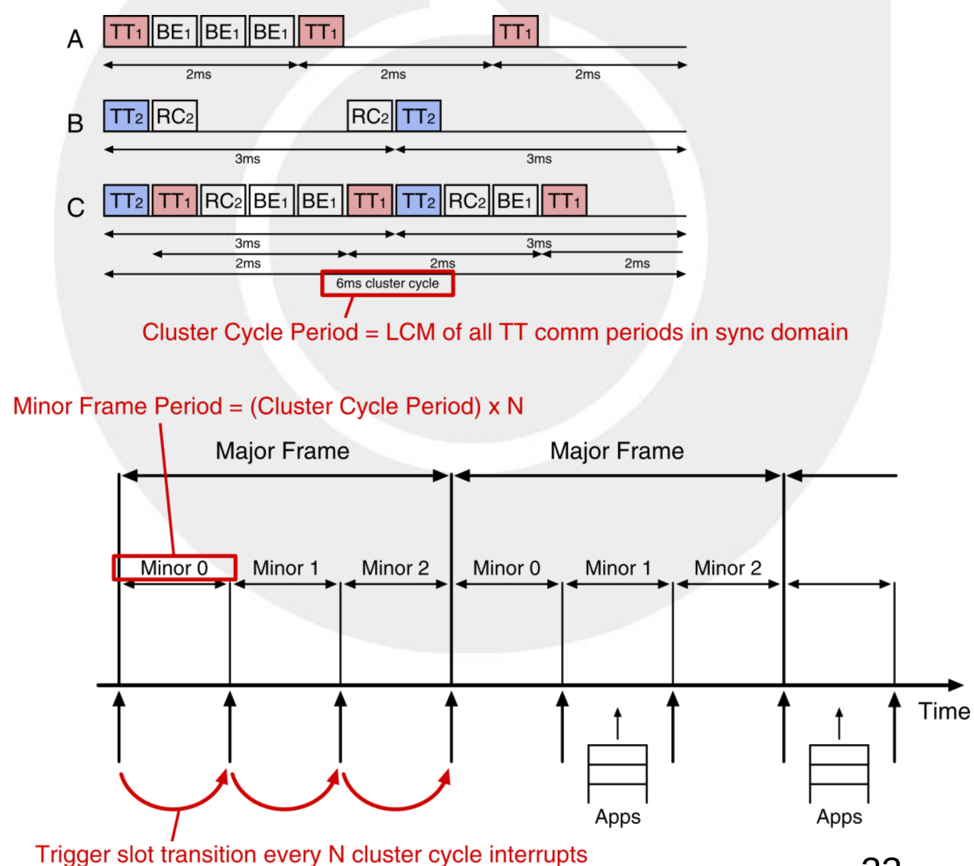


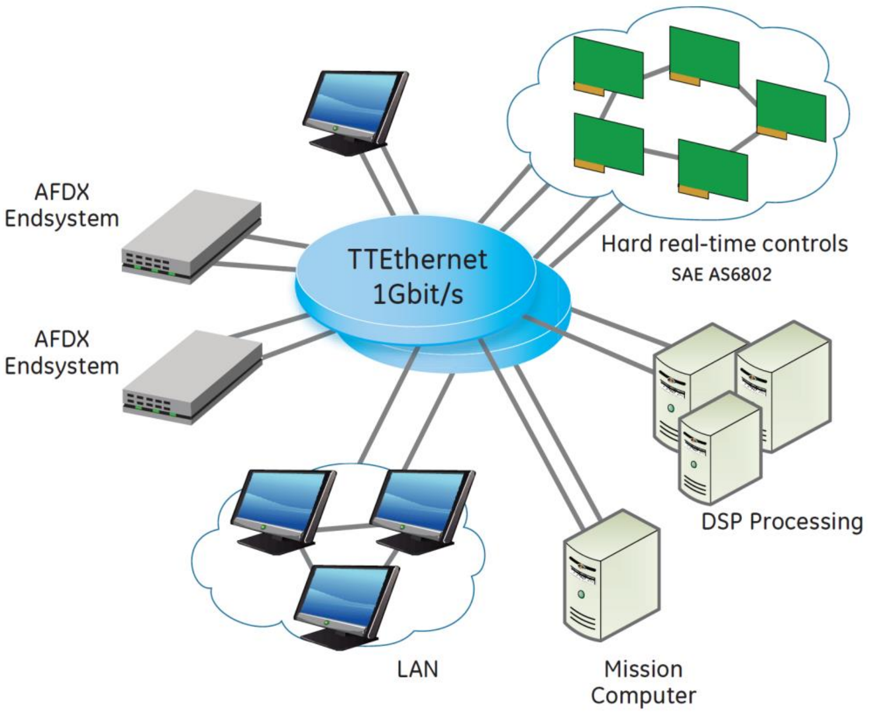
TTEthernet Library Extension throughput analysis on PC-Linux HP Z400

Network-based CFS Scheduler

Combine the concept of scheduling the execution of CFS apps with the scheduling of the TTEthernet network.

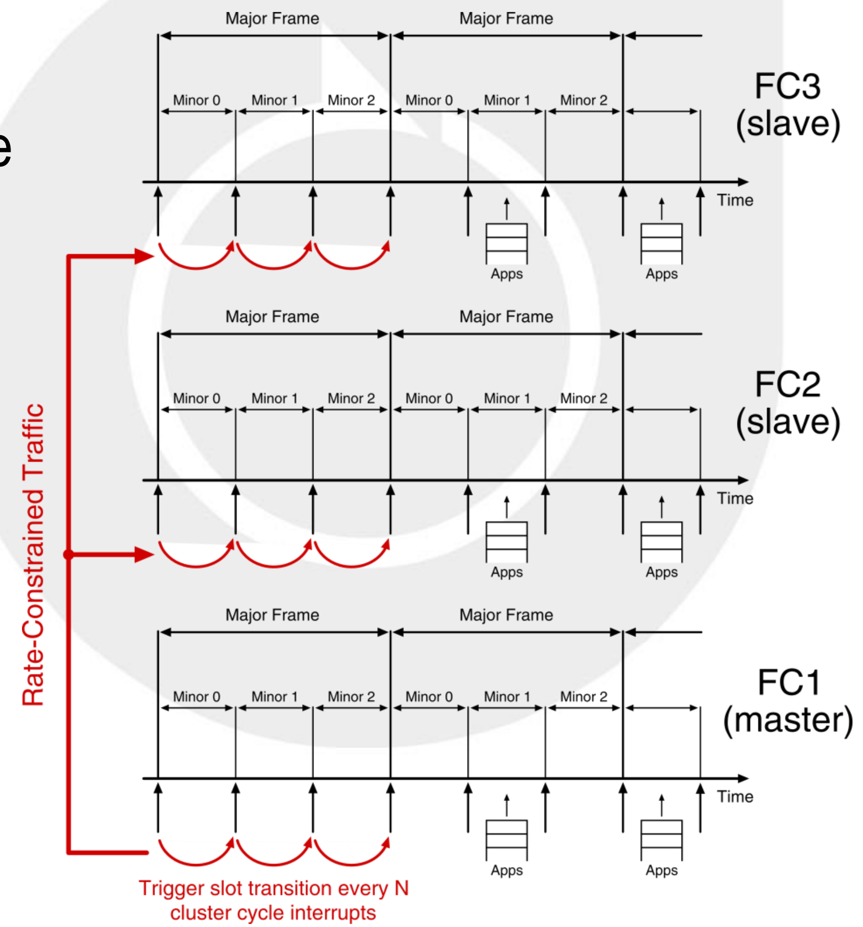
- Drives FSW execution off cluster cycle.
- Can have deterministic scheduler even on limited hardware.





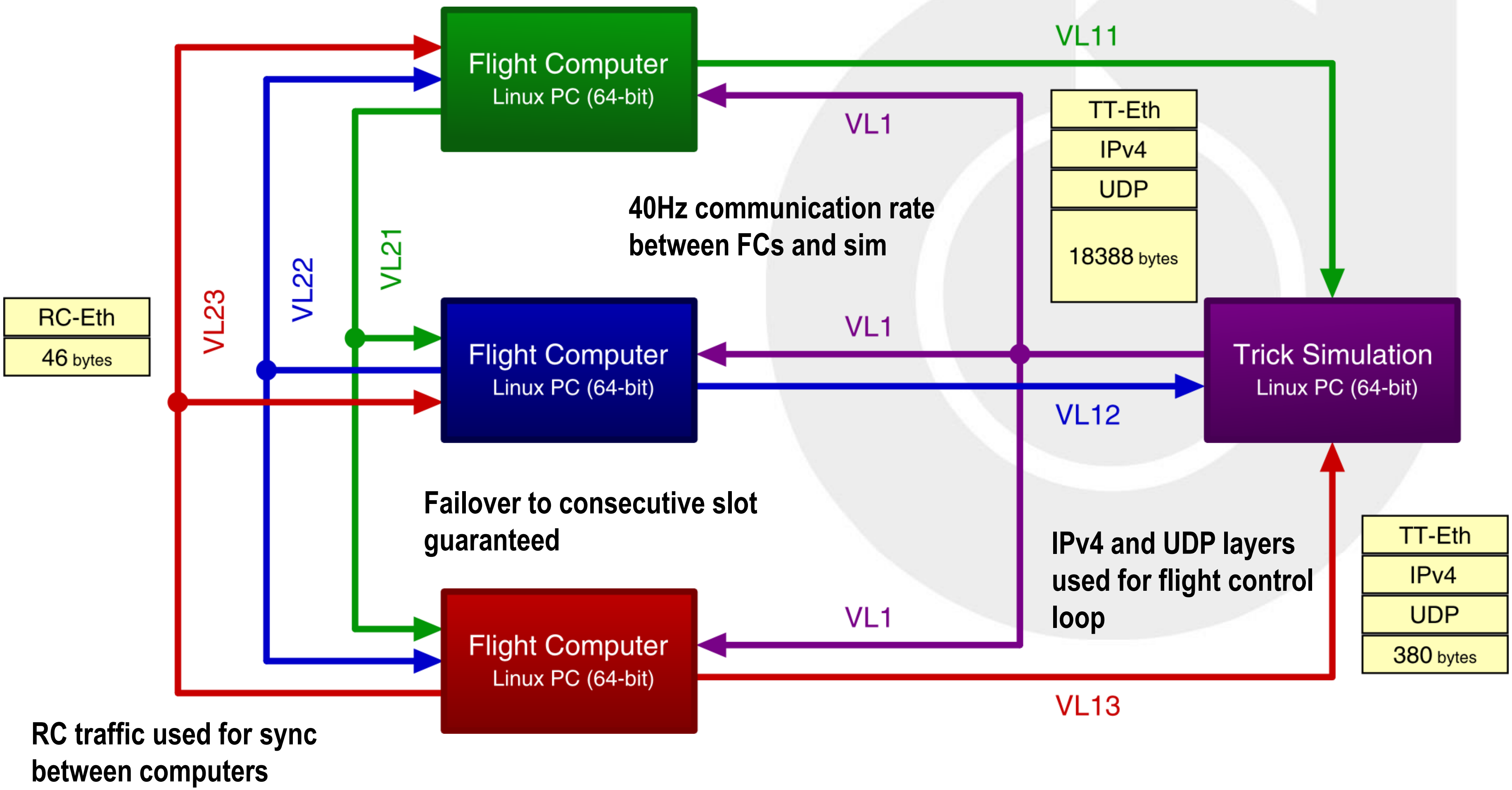
Flight Computer Synchronization

- **Message-based Synchronization**
  - Master/Slave architecture.
  - Master computer drives CFS schedule off internal or network based timer.
  - Highest-priority FC commands lower priority machines to move b/w slots.
- **Network-based Synchronization**
  - Distributed architecture.
  - Each FC drives CFS schedule off network interrupts (e.g. cluster cycle).
  - Cluster period is a global property. Interrupts are generated on each machine simultaneously.



Network-based sync in AA-2 FSW

Flight Computer Configuration



Final setup for May '15 Integrated Test at JSC (AA-2 simulation)

Shaping the Future of Aerospace